FILED
7-28-17
04:59 PM

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

Order Instituting Rulemaking Regarding Policies, Procedures and Rules for Regulation of Physical Security for the Electric Supply Facilities of Electrical Corporations Consistent with Public Utilities Code Section 364 and to Establish Standards for Disaster and Emergency Preparedness Plans for Electrical Corporations and Regulated Water Companies Pursuant to Public Utilities Code Section 768.6.	Rulemaking 15-06-009 (Filed June 11, 2015)

PACIFIC GAS AND ELECTRIC COMPANY'S (U 39-E), SOUTHERN CALIFORNIA EDISON COMPANY'S (U 338-E) AND SAN DIEGO GAS AND ELECTRIC COMPANY'S (U 902-E) JOINT COMMENTS AND CORRECTIONS TO COMBINED WORKSHOP NOTES

STEPHEN L. GARBER

Pacific Gas and Electric Company
77 Beale Street, B30A
San Francisco, CA 94105
Telephone: (415) 973-8003
Facsimile: (415) 973-5520
E-Mail: Stephen.Garber@pge.com

Attorney for:
PACIFIC GAS AND ELECTRIC COMPANY

ROBERT KANG

Southern California Edison
Law Department
2244 Walnut Grove Ave
Rosemead, CA 91770
Telephone: (626) 302-6012
Facsimile: (626) 302-6962
E-Mail: rjk555@mail.com

Attorney for:
SOUTHERN CALIFIORNIA EDISON

KEITH MELVILLE

San Diego Gas and Electric Company
8330 Century Park Court, CP32D
San Diego, CA 92123-1530
Telephone: (858) 654-1642
Facsimile: (619) 699-5037
E-Mail: KMelville@semprautilities.com

Attorney for:
SAN DIEGO GAS & ELECTRIC COMPANY

Dated: July 28, 2017

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

Order Instituting Rulemaking Regarding Policies, Procedures and Rules for Regulation of Physical Security for the Electric Supply Facilities of Electrical Corporations Consistent with Public Utilities Code Section 364 and to Establish Standards for Disaster and Emergency Preparedness Plans for Electrical Corporations and Regulated Water Companies Pursuant to Public Utilities Code Section 768.6.	Rulemaking 15-06-009 (Filed June 11, 2015)

PACIFIC GAS AND ELECTRIC COMPANY'S (U 39-E), SOUTHERN CALIFORNIA EDISON COMPANY'S (U 338-E), AND SAN DIEGO GAS AND ELECTRIC COMPANY'S (U 902-E) JOINT COMMENTS AND CORRECTIONS TO COMBINED WORKSHOP NOTES

Pursuant to the July 12, 2017 Administrative Law Judge's Ruling Issuing Combined Workshop Notes and Request for Straw Proposals ("ALJ's Ruling"), Pacific Gas and Electric Company ("PG&E"), Southern California Edison Company ("SCE"), and San Diego Gas and Electric Company ("SDG&E") (collectively "Joint Parties") timely file joint comments and corrections to the Physical Security Combined Workshop Notes attached to the ALJ's Ruling.[1/]

The Joint Parties appreciate the opportunity to submit comments and corrections to the Workshop Notes. On the whole, the notes accurately reflect both the substance and tenor of the workshops, and the Joint Parties have only minimal comments. Our limited substantive comments focus on four main areas:

- The discussion that under NERC CIP-14, utilities provide highly-sensitive information through an onsite "reading room" approach, and the corresponding discussion that the Commission may want to consider using that same model for highly sensitive information.
- The discussion that utilities and regulators will not be able to eliminate the risk of a physical attack.

1/ Pursuant to Rule 1.8(d), PG&E has been authorized to file these joint comments on behalf of SCE and SDG&E.

- The discussion that unlike CIP-14 which is designed to address the potential of a terrorist attack on critical transmission facilities that could result in grid instability, there is not the same threat on the distribution system where impacts will by definition be more localized.
- The discussion that one size does not fit all and that redundancy and resiliency can be as or more cost effective in protecting the distribution grid as physical walls and traditional defenses.

Attached to this pleading and incorporated herein are redlined corrections to the Attachment A that reflect the comments above along with self-explanatory corrections/edits.

Respectfully Submitted,

STEPHEN L. GARBER

By: */s/Stephen L. Garber*
STEPHEN L. GARBER

Pacific Gas and Electric Company
77 Beale Street, B30A
San Francisco, CA 94105
Telephone: (415) 973-8003
Facsimile: (415) 973-5520
E-Mail: Stephen.Garber@pge.com

Attorney for:
PACIFIC GAS AND ELECTRIC COMPANY

Dated: July 28, 2017

ATTACHMENT A

PG&E/SCE/SDG&E Redline Corrections/Edits to Workshop Notes

PG&E/SCE/SDG&E Redline Corrections/Edits to Workshop Notes

R.15-06-009 GK1/ek4 Attachment A

Physical Security of Electric Facilities|R.15-06-009|CPUC Safety and Enforcement Division
May 2, 2017 | Workshop 1 | 9:30 a.m. to noon
Ca/OES Offices/3650 Schriever Avenue1 Room MPR 1 & 2 / Mather1 CA

CPUC contacts: Martin Kurtovich, Senior Engineer 1-415-703-2623 *mrk@cpuc.ca.gov*
Jeremy Battis, Senior Analyst 1-415-703-3041 *jbe@cpuc.ca.gov*

W O R K S H O P A G E N D A

9:30- 10:00 a.m. **Opening Remarks by CPUC President *Michael Picker*, Commissioner *Cliff Rechtschaffen*, and Administrative Law Judge *Gerald Kelly***

10:00 – 10:15 am **Opening Remarks by Director of the Governor's Office of Emergency Services, *Mark Ghilarducci***

10:15 - 10:30 a.m. **Overview of the Proceeding, *Laying the Ground Rules for Getting It Right*, *Arthur O'Donnell, SED Risk and Safety Supervisor, CPUC***

10:30 – 10:40 am **BREAK TEN MINUTES**

10:40- 11:40 a.m. Two-part Panel Discussion

Who Needs to Know – Balancing Security with Collaboration: *Information Sharing for Critical Infrastructure Protection*

- Determining the extent to which closed door sessions are desirable and warranted
- Determining who gets access and who does not
- Recommendations on qualifying criteria for individuals and entities
- Recommendations on any appropriate new protocols

Overview of Information Categories

- Existing information categories
- Any proposed new information categories and whether existing practices are sufficient

Moderated by *Arthur O'Donnell, SED Risk and Safety Supervisor*
Panelists

- ***Scott Aaronson, Executive Director, Security and Business Continuity, Edison Electric Institute***
- ***Herb Brown, Director, Sacramento Fusion Center,***
- ***John Pespisa, Director of Compliance, SCE***
- ***Christopher Vicino, Director of Security and Emergency Management, LADWP***

11:40 - noon When to Invoke PU Code Sec. 364(d) To Protect Critical Infrastructure
Brainstorming and Consensus Exercise Facilitated by SED staff

Noon ADJOURN

OVERVIEW AND PURPOSE
Level-setting Workshop 1: Information Sharing, Protection, and Confidentiality | Establishing Proceeding Rules of Engagement for Input and Testimony on Sensitive Subjects | Establishing Protocols for Data Access and Transfer

Protection of critical infrastructure is everyone's responsibility. Yet any security measure can be rendered impotent if certain vulnerabilities are revealed to capable malicious actors. With the essential need for collaboration and partnerships across multiple organizations for critical infrastructure protection, response, and recovery, the Commission has an interest in ensuring it has in place the best possible rules, standards, protocols, and best practices for protection, disclosure, and transfer of electric utility security-related information.

This program seeks to:
A) establish consensus on ground rules for the workshop series including appropriate topics of discussion and level of detail and disclosure;
B) consider who should be invited to/excluded from attending any "closed-door" discovery session (or whether such an event is warranted);
C) provide an overview of information categories (existing or proposed);
D) develop recommendations on qualifying criteria for individuals and entities that seek access to certain sensitive information, and necessary protocols for making such information available;
E) identify any gaps or needs for new tools or practices to better enable information sharing; and,
E) distinguish when it is necessary to invoke PU Code Sec. 364(d).

A) Opening Session

CPUC President Michael Picker opened the workshop with perspective on the Metcalf episode. Attackers had good working knowledge of facility. Alarm at facility not triggered. Alarm to central command ignored. There was a theft ~~some days~~ approximately a year later at same facility. Combined, these events are troubling for what they reveal in regard to safety culture.

Additional observations put forward by Picker:

- Redundancy is built into the system— has been a primary defense deterrent.
- The CPUC is not a response agency; CPUC mission is to regulate monopolies and actually ensure no competition.
- Security threat from bad actors. How to ensure that IOUs are spending appropriate amount? How to ensure proper level of redundancy?
- The CPUC will depend on help of sister agencies to provide capabilities that do not exist at CPUC.
- Regulatory agency oversight is not always successful; Federal pipeline coordination is one example. Gas wells is an area where CPUC has little jurisdiction or knowledge (limited to a depth of 20 feet). When other agency failed; we failed. We want to ensure this experience is not repeated.
- Does the CPUC have sufficient cybersecurity protections to safely store critical infrastructure security plan information?

Assigned Commission Cliff Rechtschaffen, followed, noting that the incidents President Picker described are a wake-up call. He outlined the procedural status and expressed an interest in learning and possibly developing a consensus approach to the rulemaking.

Arthur O'Donnell, SED Risk and Safety Supervisor offered several observations, including:

- Roots of this proceeding track to a number of emergencies besides Metcalf.
- The Fresno shooting range gas pipeline dig-in incident is one.
- Metcalf was an education for us. New event; how should CPUC respond? What was CPUC responsibility?

- In the end, there was FERC/NERC purview. And CPUC investigators were relieved by FBI.
- Incident caused a ripple across power industry. Stroke or serious incident? Wake-up call.
- The Commission wrestled with how to respond. Authorized $100m to PG&E to test physical security measures.
- In responding to SB 699, the CPUC drafted a staff White Paper, made available Feb. 2015.
- Expect to update staff white paper in coming months.
- Scoping Memo for the physical security proceeding issued in March 2017.A Final Decision is expected April 2018.
- In 2017, several key first steps taken by SED staff to build knowledge base and working relationships.
- SED data request to IOUs led to responses that were varied and not always complete.
- IOUs ~~need~~ are now required to provide a cover page indicating the specific info that is confidential~~privileged~~.
- PUC Sec. 583 prevents release by CPUC of disclosure of certain info deemed confidential. This proceeding will need to accommodate that and balance need-to-know information against the public's right-to-know.

Mark Ghilarducci, CalOES, stated that in its enormity and economic might, California is practically a nation state. One primary means of State coordination with local and Federal law enforcement is by way of Fusion Centers (FC). Within a given FC, there is a mix of multiple agencies that come together to blend and share expertise.

Each state governor, he continued, was invited by the Federal government to establish such centers. California.has six: San Diego, Orange County, Los Angeles, San Francisco, and two in Sacramento including one that is a statewide amalgamator. Among other things, it advises on how to classify or restrict documents.

The range of issues treated span fire rescue to environmental threats. Management of 911 dispatch centers are shared with CPUC. With President Picker, CalOES is forging strong new bonds with CPUC. As an example, he cited the Water-Energy Nexus proceeding, which he characterized as an opportunity for coordination with the State Fire Marshall and CalFire.

B) "Who Needs to Know – Balancing Security with Collaboration: Information Sharing for Critical Infrastructure Protection."

The panel consisted of:

- Scott Aaronson, Executive Director, Security and Business Continuity, Edison Electric Institute
- Herb Brown, Director, Sacramento Fusion Center,
- John Pespisa, Director of Compliance, SCE
- Christopher Vicino, Director of Security and Emergency Management, LADWP

Arthur O'Donnell, SED Risk and Safety Supervisor, served as panel moderator

Observations and positions put forward by the panel included:

- Metcalf is not so much wakeup call as reminder. And Metcalf can be viewed as a learning exercise.
- Incident response. Industry has to be right 100 percent of time, bad actor needs be right only once.

- Critical substations and soft spots can be located via public on-line maps. Redundancy/resiliency and excess capacity is a prime defense. Although Google Maps can help bad actors to identify electricity facilities, we should not aggregate such information such that it creates a roadmap for an attack.
- There is a tension between public transparency and the need to protect sensitive information. Certain types of information (e.g., security assessments and plans) must remain confidential.~~It's a constant struggle try to explain to Feds that more sensitive data be classified.Tension between need to know and need to protect information.~~
- Under NERC CIP-014, utilities provide highly-sensitive information to auditors through an onsite "reading room" approach. Across the country, EEI is increasingly seeing a "reading room" approach used for the purposes of sharing sensitive information between utilities and regulators. The CPUC may consider using that same model for sharing highly sensitive information.
- In the post-911 milieu, there is more receptiveness among agencies to share. Right to know balances and often supersedes need to know.
- Prior to 911, Feds decided what local governments (LGs) needed to know.
- It took 15 years to get 70+ fusion centers nationwide. Suspicious activity reports. How info dispersed. Sacramento FC is unique among nation.
- There are preventive success stories you will never read about in media.
- Manmade disasters are more preventable and deferrable than natural events.
- Utilities are oftentimes protecting facilities not designed for security; every case is a retrofit. Metcalf, built in the 1950s is one example.
- Security factors ~~would~~may include climate, proximity. Desolate locations. Get various entities coordinated on emergency management. Utility corporate security staff work to keep people interested in responding properly.
- Metcalf contrarians exist and they advocate for not over or under~~ new rules~~ reacting based on a single incident.
- One fact about Metcalf: it showed how resilient the grid is. Rather than only implementing security measures, improved resiliency measures can also be used to address the potential risk of customer outages.
- Utilities welcome system that codifies and provides clarity in rules.
- The industry welcomes rational approach to regulation. Not averse to regulation per se. Security is not a one size fits all and is not a check the box exercise.

- Audits include:
  - Explicit set of requirements.
  - Steps and mitigations proposed. Third-party audits to provide verification.
  - Focus on items risk to the bulk system while allowing for resiliency improvements that did not rise to the level of top priority.

Physical Security of Electric Facilities|R.15-06-009|CPUC Safety and Enforcement Division
May 31, 2017 | Workshop 2 | 9:30 a.m. to 3:00 p.m.
CPUC Auditorium /505 Van Ness Avenue/ San Francisco1 CA

Staff contacts: Martin Kurtovich, Senior Engineer 1-415-703-2623 *mrk@cpuc.ca.gov*
Jeremy Battis, Senior Analyst 1-415-703-3041 *jbe@cpuc.ca.gov*

W O R K S H O P A G E N D A

9:30- 9:35 a.m. **Welcome and Introductions**

Topic Area #1: ***Federal Statutes and Guidelines to Address Physical Security***

Part 1: NERC National Perspective
9:35- 10:45 a.m. **Grid Security and Resilency According to the NERC**
Carl Herron – North American Electric Reliability Corporation (NERC)

10:45- 10:55 a.m. B R E A K TEN MINUTES

10:55- noon **CIP-014 | Critical Infrastructure Protection | Federal Rules Overview, Applicability, and Update on Implementation Rollout**
Darren Nielsen – Manager, Cyber & Physical Security Audits, Western Electricity Coordinating Council
Richard Hyatt – Chair WECC Physical Security Work Group, Chelan County (Washington) PUD
John Pespsia – Director of NERC Compliance, SoCal Edison

Noon- 1:15 p.m. L U N C H – one hour, 15 minutes

Part 2: California Lens Perspective
1:15- 2:00 p.m. **SMUD's Tenfold Drop in Facility Intrusions in Two Years – "*Protect Your Borders*" Paper Presentation**
James Day, Sacramento Municipal Utility District

2:00- 3:00 p.m. **Distribution System Risk and Resiliency Best Practices Discussion**
Crowdsourced brainstorming and input exercise facilitated by SED staff

A D J O U R N

OVERVIEW AND PURPOSE
Level-setting Workshop 2: State, Federal, and Industry | Standards and Responses | NERC CIP-014 and the post-Metcalf Environment

Workshop participants would receive an overview of existing Federal rules and how these may inform new State rulemaking. The North American Electric Reliability Corporation (NERC) provide the Commission and interested parties with a status report on NERC's critical infrastructure protection (CIP) standard for physical security measures. The overview of CIP-014[1] would describe facilities subject to the requirement and NERC's experience with and recommendations on its implementation.

This program seeks to:

- identify areas for State-Federal consistency;
- inform whether State-specific standards are warranted;
- identify any Federal preemptions that may limit new State-level rules;
- learn of industry response to Metcalf incident including general utility consistency or divergence across the State;
- understand utility spending, categorization, tracking, and reporting for physical security; and,
- assess emerging threats and risk outlook.

A) NERC Survey of CIP-014 Implementation

From April 2015 through August 2016, NERC physical security advisor Carl Herron conducted on-site visits to survey how entities were implementing CIP-014. His report to the NERC Board of Directors in December 2016 covered visits to 19 utilities around the country. The intent was to identify major challenges to implementation and gather more information about the physical infrastructure subject to CIP-014. "This is not so much about the standards, but about the effectiveness of the standards," Herron said.

In general, he said, entities expressed concern with timelines for implementation, but it appears that five years is a reasonable time to design and implement a security plans to meet CIP-014.

Common themes found during the survey included how the utilities dealt with these issues:

- Third-Party review;
- Defining the characteristics of facilities subject to a plan;
- Determining what data would be requested in an evaluation;
- Confidentiality of CIP-014 data – utilities retain certain information on-site;
- Challenges of multiple ownership of critical substations;
- Effecting a tiered approach to establishing priority facilities.

Assessing the potential ~~for~~ threats to physical infrastructure is dependent on various factors, a primary one being their location. Among "common characteristics" used to determine criticality noted by the NERC survey:

- Electric substations located near gas pipelines;
- Substations in high-crime areas;
- Remote/rural locations with limited law enforcement and longer incident response times;
- Facilities that support other critical infrastructure or facilities;
- Proximity to "unique threats";

- Proximity to roads and highways;
- Multiple transmission lines;
- Being located near other substations not owned by the same operator.

Coordination, both within a utility's organization and with external entities, especially law enforcement agencies, is important to implementation effectiveness. Devising security plans often requires "conversations with the engineers" and some of the survey entities worked out memorandums of understanding with state enforcement agencies to enable better protection of equipment in case of an incident.

Physical solutions vary with different kinds of security countermeasures being applied – a "one-size fits all" model will not work. Some of the common measures seen in the field included:

- Intrusion-detection systems
- Video surveillance and thermal cameras
- Physical barriers like anti-climb and anti-cut fencing
- Ballistic-resistant fencing
- Vehicle barriers and crash gates
- Gunshot-detection systems
- Additional lighting

Herron concluded that his survey indicated "The industry is addressing threats and vulnerabilities. The industry is being very aggressive in implementing CIP-014."

B) The NERC presentation was followed by a panel of utility and industry experts to further discuss the implementation of CIP-014:

Darren Nielsen, Western Electricity Coordinating Council ~~and the Los Angeles Department of Water & Power~~
Richard Hyatt, WECC and Chelan County Public Utility
John Pespisa, Southern California Edison
Arthur O'Donnell, SED Supervisor, served as moderator

Utility perspectives put forward:

- The CIP-014 standards were written to allow for ~~much~~ discretion to propose unique solutions – realized no "one-size fits all" model for physical security works due to various operational and geographical factors.

- Need to evaluate the threat and criticality of each facility. Need to proceed at the transmission level facility by facility.

- Critters and severe weather are the main culprits of power outages and linemen are the frontline of defense.

- There is a WECC working group with about 60 members that has been very effective in sharing information and resources related to physical security compliance despite the variety of points of view. "We've got 60 different people with a lot of different opinions."

- One of the valuable tools is using CARVER analysis of threat assessment.

- Doesn't believe in high-priced defenses when can keep spare parts and trained maintenance repair technicians close at hand for a half-hour response time. More sensible to give attention to supply-line management.

- NERC standards represent the basis for planning. Other trade standards exist. Would build off existing standards rather than recreating them.

- CIP-014 was developed by industry experts and adopted by NERC to specifically address the potential of a physical attack on critical transmission substations that could result in grid instability, uncontrolled separation, or cascading outage. There is not the same threat on the distribution system.

- Utilities and regulators will not be able to eliminate risk of a physical attack occurring, but actions can be taken to minimize and reduce the risk and consequences of an attack.

- The financial cost is an issue with CIP-014, as many of the physical hardening measures can be costly. Utilities need to balance customer rates with any spending on physical security. Consider focusing only on important facilities, not all facilities.

- NERC CIP regulators incorporated the Reading Room approach in CIP-014 for use in regulator audits. It's expressly built into the Standard.

- Protecting the grid can go beyond walls and traditional defenses. It can be achieved by enhancing resiliency.

- With experience the WECC audit process has become better understood, and some entities are preparing by doing "mock" audits. "We have seen audit maturity grow, and we're moving from audits that are increasingly intensive to moving the focus to internal controls."

Themes advanced by SED:

- We are exploring the CIP paradigm to determine best practices into State-level regulation. Knowing that we don't have ratesetting authority over public-owned utilities, how do we go about getting POUs to embrace the process?
- Looking at personnel and equipment sharing in the event of an emergency, should the CPUC require some evidence of robust inventory?
- Have recently tested asking IOU to put forward its own self-identified plan with assurances? Might this work here?

C) Afternoon presentation by James Day, Sacramento Municipal Utility District

The major theme of Day's presentation was the need to focus efforts to prioritize among risk areas that include: safety, reliability, brand (reputation), revenue and compliance. Knowing what you are protecting against is critical:

- Fires/explosions
- Vandalism & copper theft
- Keeping people from getting hurt

The challenge is "How do you know what to protect?"

For SMUD, it turned out that a major problem was copper theft. In 2011 there were 89 recorded intrusions at utility facilities. The utility employed a new system of wireless video cameras and other relatively low-cost measures including forming a metal theft task force and targeting metal recyclers, and was able to cut the number of incidents to just 8 in 2012.

However, aside from copper theft, Day said, "There is no clear trend. What is the threat? To the distribution system, it is pretty non-existent. We have a robust system. There is a narrow range of criticality. Some facilities have more load or more customers, some serve hospitals.

None of our distribution substations would cause load shedding, and none of our transformers went beyond R2" in the CIP-014 construct.

D) Afternoon open discussion

Much of the conversation was about how to draw on the federal CIP platform to identify what, if anythingwould be appropriately applied to distribution-level assets. Rather than try to brainstorm during the workshop, utilities offered to meet off-line to draft a "conceptual framework" that might provide the Commission with better guidance on how to assess ~~critical~~important assets at the distribution level.

The utilities agreed to draft a straw proposal for consideration during Workshop 3 on June 21.

###

Physical Security of Electric Facilities|R.15-06-009|CPUC Safety and Enforcement Division
June 21, 2017 | Workshop 3 |9:30 a.m. to 3:30 p.m.
SoCa/ Edison / 2244 Wa/nut Grove Ave./ Rosemead1 CA

Staff contacts: Martin Kurtovich, Senior Engineer 1-415-703-2623 *mrk@cpuc.ca.gov*
Jeremy Battis, Senior Analyst 1-415-703-3041 *jbe@cpuc.ca.gov*

W O R K S H O P A G E N D A

9:30- 9:35 a.m. **Welcome and Introductions**

9:35- 10:05 a.m. **What Are We Protecting Against? California Theft Intrusions Threat; Insurance Industry Stats and U.S. DOE OE-417 Electric Disturbance Event and Incident Reports**
SED staff presentation by Martin Kurtovich

10:05- 10:45 a.m. **Physical Security Assessments: Threat Vulnerability and Security and Mitigation Plans, *a Consultant Expert Perspective on CIP-014 Compliance***
Harford Field III, Corporate Risk Solutions, Inc., Manager Consulting Services

10:45- 10:55 a.m. B R E A K TEN MINUTES

10:55- 11:45 a.m. **Incident Response and Resiliency Presentation, Part I**
Emergency preparedness and response plans, IOU perspective
Thomas Jacobus, SCE, Principal Manager, Business Resiliency
Robert Kang, Senior Attorney, SCE

11:45- 1:15 p.m. L U N C H – one hour, 30 minutes

1:15- 1:45 p.m. **Incident Response and Resiliency Presentation, Part II**
Emergency preparedness and response plans, POU perspective
Stephen E. Lafond, Riverside Public Utilities, Principal Engineer in Substation, Transmission, and Distribution Standards (Energy Delivery)

1:45- 2:25 p.m. **Distribution System Risk Resiliency and Vulnerability Prevention Panel Discussion**
Spare parts inventories, dispatch, and change-outs; deployment of mobile generator units; distribution system design, redundancy, and resiliency; backup capabilities such as switching, back-ties, and load transfer; equipment and best practices sharing strategies.
Raymond Trinh, PG&E, Manager in Substation Asset Strategy and Reliability
Stephen E. Lafond, Riverside Public Utilities, Principal Engineer
Alex Salinas, SCE, Principal Manager, Technical Support
Moderated by Arthur O'Donnell, SED Risk and Safety Assessment Supervisor

2:25- 2:30 p.m. B R E A K FIVE MINUTES

2:30- 3:30 p.m. **Utility Straw Proposal**
Presentations by the utilities and discussion

3:30 p.m. A D J O U R N

Overview

Workshop 3, held June 21, at SoCal Edison's Rosemead headquarters, aimed to provide the Commission and its staff with a better understanding of the industry's response to CIP-014 rules, how the rules were intended to address particular threats, how CIP-014 may be appropriate as a model for new state-specific rules, and California utilities' receptiveness to cooperating with CPUC staff to propose a set of California standards that would respond to the threat concerns and call for solutions outlined in SB 699.

After presentations about trends seen in data collected by the US Department of Energy via OE- 417 reports, and a consultant presentation on designing physical security for distribution facilities, representatives of Southern California Edison presented on the utility's business resiliency effort, the Riverside Public Utilities representative reported on how the city's emergency planning process resulted in upgrades to a critical substation and the results, and a panel discussed various ideas for addressing physical security threats, ~~and improved reliability to~~ including an examination of redundancy and/or resiliency of distribution level assets.

The afternoon discussion was presented two alternative "straw proposals" for a common framework to guide utility plans for physical security and the CPUC assurance of adequacy.

A) **"What are We Protecting Against?" CPUC Presentation on Physical Security Performance Rating System** by Martin Kurtovich PE, Senior Engineer, CPUC

SED staff offered a comparison of existing Federal and State electric industry physical security incident reporting methods and associated databases ~~--~~ US Dept. of Energy Reporting Form OE-417 and CPUC Incident Report Form – to the insurance industry's physical security metrics and performance rating system. The existing US Dept. of Energy ~~and CPUC reporting~~ system~~s are~~ is limited in scope and applied resources and ~~are~~is triggered by events that impact or may impact the Bulk Electric System.~~major outages only.~~ The CPUC reporting criteria is limited to major outage events, property damage over a certain threshold, media attention, and serious injury or death from electric contact.

Retrieving information from these systems is cumbersome and of limited benefit. The insurance industry version appears to have superior metrics for metal theft, is readily available, allows for analysis, and reflects physical security performance. SED staff noted that the utility straw proposals as submitted did not describe any means for measuring utility performance.

B) **"Physical Security Assessments: Threat Vulnerability and Security and Mitigation Plans, a Consultant Expert Perspective on CIP-014 Compliance"** Harford Field III, Corporate Risk Solutions, Inc.

Mr. Field's presentation on security risks associated with electric facilities noted that unlike cyber threats, physical security attacks in the United States have been infrequent, have typically resulted in nominal damage and relatively negligible cost, and have not evidenced organized coordination. To date, consequences of these attacks have been negative publicity, additional regulatory burden, and significant cost of hardening physical assets.
Field listed the primary "likely threats" of a physical asset attack:

- Insider threat
- High-powered rifle
- Improvised explosive device carried by a vehicle or individual

He added that the existing threat of significant destruction is a threshold of 50 pounds of TNT carried by an individual's own capacity and detonated from a distance of 1,800 feet. An emerging and growing threat are drones operated by malicious actors; today's drones are capable of delivering a five-pound payload, which could describe a typical pipe bomb.

He reminded the Commission and stakeholders that CIP-014 standards were intended to address the threat of a military-grade coordinated terrorist attack, which to date has not found an energy sector target on US soil.

He joined previous speakers in restating that the electric distribution system is not attractive as a terrorist target and that other physical security challenges are associated with distribution assets. Mr. ~~Hill~~Field added that, if a physical attack on a distribution level substation did occur, there may be an impact at the local level, however the distribution system has redundancy and resiliency to support reliability. He offered alternative approaches to physical hardening including Crime Prevention Through Environmental Design (CPTED) and the Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP uses a common methodology for planning and conducting individual emergency preparedness exercises. This methodology applies to exercises in support of all national preparedness mission areas.

A common methodology ensures a consistent and interoperable approach to exercise design and development, conduct, evaluation, and improvement planning.

C) **SCE Incident Response and Resiliency Presentation** by Thomas Jacobus, SCE Principal Manager, Business Resiliency, and Robert Kang, SCE Senior Attorney

This informative presentation addressed the range of efforts that Southern California Edison (SCE) has undertaken related to physical security, including annual exercises with FBI, DHS, and CPUC to practice drill various types of physical security incidents.

D) **Riverside Public Utilities Resiliency Presentation** by Stephen E. Lafond, Principal Engineer

Riverside Public Utilities described its emergency planning program, which includes analysis of projects to upgrade physical security at substations facilities. Riverside incident response and resiliency approach is informed and prompted by the Federal Disaster Mitigation Act of 2000. The City of Riverside develops a Local Hazard Mitigation Plan to meet federal requirements.
The plan also enables the City to apply for federal disaster preparation assistance. The plan is then reviewed and adopted by 1) its local governance (City Council); 2) Riverside County Office of Emergency Services; 3) California Office of Emergency Services; and 4) the Federal Emergency Management Administration (FEMA). Riverside's Critical Infrastructure Protection Program follows the National Infrastructure Protection Program.

For added resiliency, Riverside Public Utilities has portable substations and switch gear on hand in the event there is a failure in any of their 14 substations. In the event of equipment failure, these portable units are temporarily installed and operated while a new replacement unit is ordered from the manufacturer.

E) **Distribution System Risk Resiliency and Vulnerability Prevent Panel Discussion**
Raymond Trinh, PG&E, Manager in Substation Asset Strategy and Reliability
Stephen E. Lafond, Riverside Public Utilities, Principal Engineer
Alex Salinas, SCE, Principal Manager, Technical Support Moderated by
Arthur O'Donnell, SED Supervisor

The panel format encouraged participants to share the perspective of POUs and IOUs on risk and vulnerability for distribution assets. SCE noted that prescriptive regulation is a concern.
SCE company goals include resiliency as a focus for its system, including the distribution system. SCE and PG&E prefer~~s~~ to address physical security through a resiliency approach which means that physical security measures are broader than just physical hardening of substations. Rewiring of circuits that improve operational flexibility is one example where ~~physical security is enhanced while~~ the distribution system is made more resilient.

Each of the utilities emphasized that ensuring resiliency of the distribution system is an effective counter to any prescriptive approach that focuses solely on "hardening the system" at a high cost. They discussed how they provide for adequate back-up equipment replacements – including mobile transformers -- and arrangements with vendors to expedite replacements, when necessary.

E) Utility Straw Proposals

Two straw proposals were shared with the service list prior to the workshop. One joint proposal, led by SCE, appears to have the support of PG&E and small, rural, and publicly-owned utilities. A second straw proposal has been put forward by SDG&E. The SCE/PGE/POU proposal was based on current CIP 14 methodology and allows flexibility by allowing utilities to select the methodology that best fits that utility's needs.

The straw proposals were provided for informal discussion purposes. Formal proposals would need to be reviewed and approved by the parties' leadership.

The discussion of the Utility Straw Proposal in Workshop 3 mainly consisted of SCE describing how it slightly modified an earlier proposal in response to SED staff comments, and SDG&E proposing an alternative version.

The major difference between the two versions is SDG&E's Section 2, which describes "risk based performance standards" and a tier system for categorizing which assets might be highest priorities. SDG&E's proposal also would not incorporate the use of a third-party evaluator. Where the SCE (joint utility) version proposed creation of a Distribution Substation and Distribution Control Center Security Program DSDCCSP), SDG&E instead proposes Electric Distribution Site Security Plan that describes the risk-based analysis of facilities, and a Distribution Security Program (same function as the DSDCCSP). SDG&E's conceptual proposal is based on the chemical industry protocol.

SCE changed the language about prescribing "reading room" access to confidential documents, no longer limiting it to Operator headquarters, but to a "mutually agreed-upon location" which could be the utility's local offices; SDG&E retained the company headquarters restriction. The POUs listed some of their issues, but generally appeared on board with an approach that would have the Commission cast less direct oversight over the POUs' security plans, than the IOUs'. In return for the Commission taking this "light touch" approach to the POUs, the POUs would provide some mechanism of assurance that a) they have a plan, and b) it's been vetted by a knowledgeable entity. POU respondents noted their concern about "extent and scope" of any third-party or CPUC audit of plans. Another concern raised related to a possibility that new requirements for physical security or resiliency might change relationships between utilities and their customers, especially regarding expectations of service.

As described previously, Riverside Public Utilities described its emergency planning program, which included analysis of projects to upgrade physical security at substations facilities. Riverside's planning program is reviewed and signed off by FEMA, as well as its local Riverside Public Utility governing authority (City Council and Board of Public Utilities). SED staff suggested that such a process might be sufficient to satisfy the Commission's need for assurance and appears to be consistent with the Straw Proposal's existing IOU-POU bifurcation approach (Section 4 in the SCE version).

Participants discussed steps leading to a proposed physical security framework that 1) identifies threats, 2) specifies criteria to identify ~~critical~~important distribution facilities, and 3) enables individual utilities to determine appropriate mitigation measures.

Discussion ended with conversation on next steps. There was discussion of allowing another iteration of a common straw proposal by the utilities in an effort to bridge differences and arrive at a single unified proposal that all California electric utilities could support. To accommodate this extra effort, SED staff will consider altering the expected schedule of remaining workshops to allow more time for consideration of a revised proposal.

(End of Attachment A)